

(51) Int.Cl.*	識別記号	序内整理番号	F I	
G 0 6 F 7/58		7522-5E	G 0 6 F 7/58	B
G 1 1 B 20/12	1 0 2	9295-5D	G 1 1 B 20/12	1 0 2
20/18	5 4 4	9558-5D		5 4 4 A
	5 7 0	9558-5D		5 7 0 B
H 0 3 M 13/22		8732-5K	H 0 3 M 13/22	
			審査請求 未請求	予備審査請求 未請求(全30頁)

(21)出願番号	特願平8-523383
(86) (22)出願日	平成8年(1996)1月29日
(85)翻訳文提出日	平成8年(1996)10月1日
(86)国際出願番号	PCT/IB96/00077
(87)国際公開番号	WO96/24098
(87)国際公開日	平成8年(1996)8月8日
(31)優先権主張番号	95200242.6
(32)優先日	1995年2月1日
(33)優先権主張国	オランダ(NL)
(31)優先権主張番号	95200520.5
(32)優先日	1995年3月3日
(33)優先権主張国	オランダ(NL)

(71)出願人	フィリップス エレクトロニクス ネムロ ーゼ フエンノートシャップ オランダ国 5621 ベーアー アンドー フェン フルーネヴァウツウェッハ 1
(72)発明者	ホールマン ヘンドリク ドリク ロデウ エイク オランダ国 5621 ベーアー アンドー フェン フルーネヴァウツウェッハ 1
(72)発明者	バッヘン コンスタント ポール マリー ヨゼフ オランダ国 5621 ベーアー アンドー フェン フルーネヴァウツウェッハ 1
(74)代理人	弁理士 杉村 晓秀 (外6名) 最終頁に続く

## (54)【発明の名称】順列ユニットを含む回路配置及び一団の項目を処理する方法

## (57)【要約】

この回路配置は番号の集合の疑似ランダム順列を計算する。該回路配置により計算されることのできる順列は、幾つかの基本的疑似ランダム順列の結合及び計算された順列の逆順列を含むことを要する。(結合とは累積的に繰り返される番号の順序変更に対応し、逆順列とは或る順列を元に戻すところの順列である。) 基本的疑似ランダム順列、その結合、及び逆順列はすべて同じ生成器により計算され、該生成器の動作は整係数 $\alpha$ の或る集合を特定することにより適切な順列を計算することが命令される。該生成器は、 $\alpha$ を $m$ のすべての素因数で整除される整数の番号で、もし $m$ が4の倍数ならば $\alpha$ も4の倍数であり、そのポテンシーアル $s(\alpha)$ は2以上であるとするとき、 $I$ に対応して $n=0, \dots, m-1$ なる番号 $n$ の順列 $\sigma(n)$ を計算する。すべての順列に同じ $\alpha$ が用いられとき、生成された順列のすべての結合及び逆順列は同じ生成器により同じやり方で計算できると仮定する。第1及び第2の順序はいずれもこのタイプの異なる順列に対応するとし、項目の一団を記憶媒体中に第1の順序で記憶し、該記憶媒体から第2の順序で検索することにより、上記一

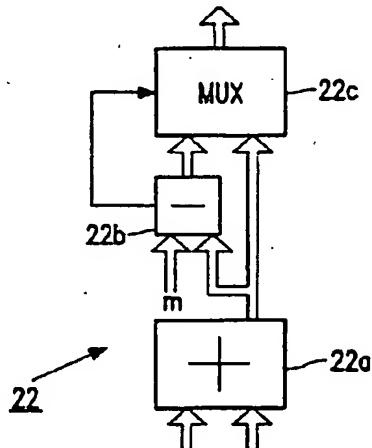


FIG. 4

## 【特許請求の範囲】

1. 一组のm個の番号の逐次順列生成する回路配置において、  
該回路配置は：

- 一 制御信号を生成するための制御手段を有して成り、各制御信号は、sを1  
より大きい自然数とするとき、 $f_i$  ( $i=0, \dots, s$ ) という  $(s+1)$  個の整系数のそれ  
ぞれの一組を特定するものであり、また

一 各サイクルが上記制御信号の1つにそれぞれ制御される繰り返しサイクル  
で動作する計算手段を有して成り、該計算手段は、

- $f_i$  を上記制御信号の1つによりそれぞれ特定された整系数とし； $\alpha$  を全サイク  
ルに共通の整数の番号とし、 $\alpha$  はmのすべての素因数で整除され且つmに關し、  
に等しいボテンシーアルゴリズムを持つ；とするとき、

$$\alpha(n) = x_0 + \sum_{i=1}^{s-1} x_i \left[ \frac{n}{f_i} \right] \alpha^{i-1} \bmod m$$

に対応する逐次順列のそれぞれ1つを、上記サイクル中に計算するものである  
ことを特徴とする回路配置。

## 2. 請求項1に記載の回路配置において、

上記制御信号のうち少なくとも1つは、 $(s+1)$  個の整系数による順列が、逐  
次順列のうちから少なくとも2つの順列を結合したものに対応するように、該  $(s  
+1)$  個の整系数を特定することを特徴とする回路配置。

3. 請求項1又は2に記載の回路配置において、もし  $m$  が4の倍数なら、 $\alpha$  も4  
の倍数であることを特徴とする回路配置。

4. 請求項1、2又は3に記載の回路配置において、ボテンシーアルゴリズムは2であるこ  
とを特徴とする回路配置。

5. 請求項1ないし4のうちのいずれか1項に記載の回路配置において、整系数  
のそれぞれの組のうち少なくとも1つでは、 $f_0$  を除くすべての  $f_i$  が互いに等しく  
且つ  $m$  との最大公約数は1であることを特徴とする回路配置。

6. 請求項1ないし5のうちのいずれか1項に記載の回路配置において、  
上記計算手段は、各サイクル中の逐次順列番号を、中間変数  $u(i)$  ( $i=0, \dots$

,  $s$ ) から、逐次ステップ  $n$  ( $n=0, \dots, m-1$ ) で計算するように設定されて成り、

中間変数  $u(0)$  は、各サイクルの始めのステップの最初の1つで、初期化し  
て  $f_0$  とされ、

中間変数  $u(i)$  ( $i=1, \dots, s-1$ ) は、上記ステップの最初の1つで、初期化し  
て

$$u(i) = f_i \alpha^{i-1}$$

とされ、

$u(i)$  を除く各中間変数  $u(i)$  の値は、上記ステップの最初の1つを除く各逐  
次ステップで、先行ステップ中の中間変数のそれぞれのモジュロ和

$$u(i) + u(i+1) \bmod m$$

によって置き換えられ、

逐次ステップ  $n$  ( $n=0, \dots, m-1$ ) における中間変数  $u(0)$  の値は、順列置換され  
た番号  $\alpha(n)$  として用いられる

ことを特徴とする回路配置。

## 7. 請求項6に記載の回路配置において、

各々がそれぞれのメモリエレメント及びそれぞれのモジュロ加算器を含む  $s$   
個の再帰ユニットを継つなぎにして成り、  
継つなぎの先頭の再帰ユニットの上記それぞれのモジュロ加算器は、該先頭  
の再帰ユニットのそれぞれのメモリエレメント及びもう1つ別のメモリエレメン  
トに結合する1目の被加数入力を待ち、  
先頭の再帰ユニットを除く各特定の再帰ユニットの上記それぞれのモジュ  
ロ加算器は、該特定の再帰ユニットのメモリエレメントに結合する1番目の被加数  
入力と、継つなぎの中で該特定の再帰ユニットの1つ前の再帰ユニットのメモリ  
エレメントに結合する2番目の被加数入力と、を待ち、

各再帰ユニット中のそれぞれのモジュロ加算器の総和出力は、該再帰ユニッ  
トのそれぞれのメモリエレメントの入力に接続され、  
上記計算手段は、継つなぎの最終の再帰ユニット中のメモリユニットの内容  
を各サイクルの始めに初期化して  $f_0$  し、また、継つなぎの最終の再帰ユニッ  
ト

トに順次先行する再帰ユニット中のメモリユニットの内容をそれぞれ初期化して

$$f_i \alpha^{i-1} \quad (i=1, \dots, s-1)$$

とするように設定され、

もう1つのメモリユニットは初期化して  $f_i \alpha^{i-1}$  とされ、

逐次ステップ  $n$  ( $n=1, \dots, m$ ) では毎回、最終の再帰ユニットのメモリユニット

トが、ランダム番号  $\sigma(n)$  をその逐次ステップで出力する

ことを特徴とする回路配置。

8. 請求項1ないし7のうちのいずれか1項に記載の回路配置において、  
メモリを有して成り、 $m$  個の番号の組に属するところの番号は該メモリ中の  
それぞれの位置を表すアドレスに対応し、また  
各特定のサイクルでそれぞれ一組のデータ項目をメモリに書き込み、該特定  
のサイクルに後続する逐次サイクルの1つで上記それぞれ一組のデータ項目をメ  
モリから読み出すための読み出し／書き込みユニットを有して成り、上記それぞ  
れ一組のデータ項目はその特定サイクル用に生成された順列に対応するアドレス  
の順番で書き込まれ、後続サイクル用に生成された順列に対応するアドレスの順  
番で読み出される

ことを特徴とする回路配置。

9. 請求項8に記載の回路配置において、上記特定サイクル用に計算された順列  
の逆順列と上記後続サイクル用に計算された順列との結合が、該特定サイクルと  
は独立の通常の順列に等しくなるように、整係数  $f_i$  の組が選定されることを特  
徴とする回路配置。

10. 請求項8又は9に記載の回路配置において、符号器を含み、該符号器は上記  
一組のデータ項目を誤り訂正器で構成するものであることを特徴とする回路配  
置。

11. 請求項8又は9に記載の回路配置において、誤り訂正器を含み、該誤り訂正  
器は、上記のデータ項目にそれが読み出された順序で与えられた誤り訂正符号に  
従って上記一組のデータ項目を訂正するものであることを特徴とする回路配置。

12.  $m$  個の項目の一組を処理する方法であつて、 $f_0$  を除くすべての  $f_i$  が互いに等

との該一組を受け取る段階、

一 各特定の項目に、該特定の項目の上記第1順位番号の第1関数に従って、

記憶媒体内のそれぞれの位置を割り当てる段階、  
一 各特定の項目を、記憶媒体内でそれに割り当られたそれぞれの位置に記  
憶する段階、

一 第2順位番号を、記憶位置の第2関数に従って各記憶位置に割り当てる段  
階、

8. 請求項1ないし7のうちのいずれか1項に記載の回路配置において、

一 記憶媒体から項目を検索する段階、及び  
一 特定の記憶位置から検索された上記特定の項目を、該特定の位置の第2順  
位番号に従って処理する段階

を含んで成る方法において、

$n1$  を順位番号とし、 $n2$  を記憶位置の順序での記憶位置の位置番号とし； $f_i$  及  
び  $g_i$  ( $i=0, \dots, s$ ) を各々が  $(s+1)$  個の整数からなるそれぞれの集合に属する整  
数とし； $\alpha$  を  $m$  のすべての素因数で整除される整数の番号とし、 $\alpha$  は  $m$  に関し  
 $s$  に等しいボテンシーを持つとき、上記第1関数及び第2関数はそれぞれ

$$\text{location}(n1) = f_0 + \sum_{i=1}^s f_i \begin{bmatrix} n1 \\ 1 \end{bmatrix}_{\alpha^{i-1}} \bmod m$$

$$\text{ranknumber}(n2) = g_0 + \sum_{i=1}^s g_i \begin{bmatrix} n2 \\ 1 \end{bmatrix}_{\alpha^{i-1}} \bmod m$$

に対応して計算されることを特徴とする方法。

13. 請求項12に記載の方法において、もし  $m$  が 4 の倍数なら、 $\alpha$  も 4 の倍数であ  
ることを特徴とする方法。

14. 請求項12又は13に記載の方法において、ボテンシー  $s(\sigma)$  は 2 であることを  
特徴とする方法。

15. 請求項12、13又は14に記載の方法において、 $f_0$  を除くすべての  $f_i$  が互いに等

しく且つ $m$ との最大公約数は1であることを特徴とする方法。

16. 請求項12ないし15のうちのいずれか1項に記載の方法において、各サイクル中で逐次順列置換される番号 $s(\sigma)$ は、中間変数 $u(i)$  ( $i=0, \dots, s$ ) から、逐次ステップ $n$  ( $n=0, \dots, m-1$ ) で計算され、中間変数 $u(0)$ は、各サイクルの始めのステップの最初の1つで、初期化して $f_0$ とされ、中間変数 $u(i)$  ( $i=1, \dots, p-1$ ) は、上記ステップの最初の1つで、初期化して

$$u(i) = f_i \alpha^{i-1}$$

とされ、

$u(i)$ を除く各中間変数 $u(i)$ の値は、上記ステップの最初の1つを除く各逐次ステップで、先行ステップの中間変数のそれぞれのモジュロ和

$$u(i) + u(i+1) \bmod m$$

によって置き換えられ、

逐次ステップ $n$  ( $n=0, \dots, m-1$ )における中間変数 $u(0)$ の値は、順列置換された番号 $\sigma(n)$ として用いられる

ことを特徴とする方法。

#### 【発明の詳細な説明】

順列ユニットを含む回路配置及び一回の項目を処理する方法

本発明は、一組の $m$ 個の番号の逐次疑似ランダム順列(successive pseudo random permutations)を生成する回路配置に関する。

疑似ランダム順列は種々の用途を持つ。それは、誤り訂正符号と組み合わせてインターリービングの目的で用いることができ、それにより符号からのシンボルを処理する順番を変えて、システムティックな誤りに対し更に強固な誤り防護プロセスとするのである。

単数又は複数の同じ基本的疑似ランダム順列の様々な結合(compositions)により、引き続く幾つかの異なる疑似ランダム順列を生成することが望ましい、という場合はしばしばある。

例えば、もし一組の項目の順序を変えたいと欲するなら、先ずそれらの項目を記憶媒体内の記憶位置に或る順番で書き込み、次にそれらを前と異なる記憶位置の順番で記憶媒体から取り出すのである。複数の組の項目の順序変更を引き続いた行わなければならないときに記憶スペースを節約するため、先行の組が完全に読み出される以前にでも、前の組の項目が検索されて空きになった順序で、それらの記憶位置に後の組の項目を毎回記憶させたい。各組が同じ疑似ランダム順列でなければならぬならないなら、これは、引き続く各組を記憶する記憶位置の順序が前の組の記憶位置の順序にその疑似ランダム順列を結合したものでなければならない、ということを意味する。

上記回路配置は、これらの逐次疑似ランダム順列を生成しなければならないしかし、すべての必要な疑似ランダム順列を生成することは、極めて複雑な時間の掛かる演算を要求されることになろう。生成することのかなり簡単な基本的疑似ランダム順列を用いる場合といえども、そのような基本的疑似ランダム順列の結合を生成することの必要性は、種々の疑似ランダム順列の計算がその複雑さにおいて大幅に異なり、計算時間や所要のハードウェアの極めて高価なことが明らかになるであろうことを意味する。

とりわけ、本発明の目的は、単数又は複数の同じ基本的疑似ランダム順列の結

合である複数の疑似ランダム順列を生成できる回路配置を提供することであり、この回路配置は、一連の同じ計算ステップを実行するのに使われる同じ計算回路を用いて、これらの疑似ランダム順列の各々を生成することができ、必要な計算回路は簡単な構造のものである。

本発明のもう1つの目的は、項目を処理する順番が、項目を受け取る順番の疑似ランダム順列となるよう、項目を処理する方法を提供することであって、該順列は項目を記憶媒体に記憶し、記憶媒体から検索することにより達成され、所要の記憶媒体は減らす、というものである。

本発明による回路配置は、

一 制御信号を生成するための制御手段を有して成り、各制御信号は、 $s$ を1より大きい自然数とするとき、 $f_i$  ( $i=0, \dots, s$ ) という  $(s+1)$  個の整系数のそれぞれの一組を特定するものであり、また

一 各サイクルが上記制御信号の1につきそれぞれ制御される繰り返しサイクルで動作する計算手段を有して成り、該計算手段は、

$f_i$  を上記制御信号の1つによりそれぞれ特定された整系数とし； $\alpha$ を全サイクルに共通の整数の番号とし、 $\alpha$ は  $m$  のすべての素因数で整除され且つ  $m$  に關しに等しいポテンシー  $s(\alpha)$  を持つ；とするとき、

$$\sigma(n) = x_0 + \sum_{i=1}^s x_i \left[ \frac{f_i}{\alpha} \right]_{\alpha}^{s-1} \bmod m$$

に対応する逐次順列のそれぞれ1つを、上記サイクル中に計算するものであることを特徴とする。数  $\alpha$  の  $m$  に関するポテンシー  $s(\alpha)$  とは、

$$\alpha \cdot s = 0 \bmod m$$

となる最小の自然数と定義される、すなわち  $\alpha$  の  $s$  乗幕が  $m$  で整除される最小の自然数のことである。

本発明は、本発明により生成される順列  $\sigma(n)$  が数学的概念における「群」を形成する、という認識に立脚する。このことは、もし或る基本的疑似ランダム順列が、その各々を一組の整系数  $f_i$  ( $i=1, \dots, s-1$ ) は、

きるとしたら、その場合にはこれら的基本的疑似ランダム順列のすべての結合、

及びその逆順列さえもが、その各々を整系数  $f_i$  の別のそれ自身の組で特定することにより計算できる、ということを意味する。

本発明はこの認識を利用する計算手段を設けて、この計算手段により所与の公式(formula)に対応する順列を計算し、また、整系数  $f_i$  の他の組の組の特定を毎回制御して、他の順列を計算手段を再使用する。こうして、ある範囲の順列と、それらの結合と、それらの逆順列とが、同一の計算手段で順次計算でき。

本発明による回路配置の一実施例では、上記制御信号のうち少なくとも1つは  $(s+1)$  個の整系数による順列が、逐次順列のうちから少なくとも2つの順列結合したものに対応するように、該  $(s+1)$  個の整系数を特定する。

本発明による回路配置の一実施例では、ポテンシー  $s$  は2である。このやり方で計算手段の複雑さを最小のものとしてもなお、疑似ランダム順列を合理的に生成できる。しかし更によりランダム性を考慮するならば、更に高いポテンシー、例えば3以上の(4, 5等)ポテンシーが好適な場合もあるう。

本発明による回路配置の一実施例では、整系数のそれぞれの組のうち少なくとも1つでは、 $f_0$  を除くすべての  $f_i$  が互いに等しく且つ  $m$  の最大公約数は1であることを特徴とする。これにより、選択することに容易な( $f_0$  は任意である)基本的順列が提供される。このやり方で生成された順列のそれ自身による結合

$(\sigma(n)), \sigma(\sigma(n)), \dots, \sigma(\sigma(\sigma(n)))$  等々)に対応する更に多くの順列、及びこの順列の逆順列が求められる。一般的には、このやり方で求められた順列は、このように簡単な系数  $f_i$  の組で特定されないであろう。従って係数  $f_i$  で特定される等しない他の順列が、少なくとも1つこのそれぞれの順列の組に関連して使われるこことになろう。

本発明による回路配置の一実施例では、上記計算手段は：各サイクル中の逐次順列番号を、中間変数  $u(i)$  ( $i=0, \dots, s$ ) から、逐次ステップ  $n$  ( $n=0, \dots, m-1$ ) で計算するように入力され成り；中間変数  $u(i)$  は、各サイクルの始めのステップの最初の1つで、初期化して  $f_0$  とされ；中間変数  $u(i)$  ( $i=1, \dots, s-1$ ) は、上記ステップの最初の1つで、初期化して

$u(i) = f_{i-1} \alpha^{i-1}$

$u(i) \neq f_{i-1} \alpha^{i-1}$  を除く各中間変数  $u(i)$  の値は、上記ステップの最初の 1つを除く各逐次ステップで、先行ステップ中の中間変数のそれぞれのモジュロ和

$$u(i) + u(i-1) \bmod m$$

によって置き換えられ；逐次ステップ  $n$  ( $n=0, \dots, m-1$ ) における中間変数  $u(i)$  の値は、順列置換された番号  $\alpha(n)$  として用いられる；ことを特徴とする。このやり方で、順次に順列置換された値  $\alpha(n)$  の計算に掛け算を必要としないで、順列を計算することができる。掛け算を実行する回路は複雑で時間の掛かるものだから、このことは順列の計算を更に簡単に速いものとする。

本発明による回路配置のもう 1 つの実施例では、該回路配置は：各々がそれぞれのメモリエレメント及びそれぞれのモジュロ加算器(modulo adder)を含む  $s$  個の再帰ユニット(recursion unit)を縱つなぎに有して成り；縦つなぎの先頭の再帰ユニットの上記それぞれのモジュロ加算器は、該先頭の再帰ユニットのそれぞれのメモリエレメント及びもう 1 つ別のメモリエレメントに結合する 1 番目の被加数入力を持ち；先頭の再帰ユニットを除く各特定の再帰ユニットの上記それぞれのモジュロ加算器は、該特定の再帰ユニットのメモリエレメントに結合する 1 番目の被加数入力と、縦つなぎの中で該特定の再帰ユニットの 1 つ前の再帰ユニットのメモリエレメントに結合する 2 番目の被加数入力と、を持ち；各再帰ユニット中のそれぞれのモジュロ加算器の総和出力は、該再帰ユニットのそれぞれのメモリエレメントの入力に接続され；上記計算手段は、縦つなぎの最終の再帰ユニット中のメモリユニットの内容を各サイクルの始ために初期化して  $f_0$  とし、また、縦つなぎの最終の再帰ユニットに順次先行する再帰ユニット中のメモリユニットの内容をそれぞれ初期化して

$$f_{i-1} \alpha^{i-1} \quad (i=1, \dots, s-1)$$

とするようにより設定され；もう 1 つのメモリユニットは初期化して  $f_{s-1}$  とされ；逐次ステップ  $n$  ( $n=1, \dots, m$ ) では毎回、最終の再帰ユニットのメモリユニットが、ランダム番号  $\alpha(n)$  をその逐次ステップで出力する；ものとする。一組のデータ項目を、或る順番でメモリに書き込み、統いてそれらを別の順番でメモリから読み出すことによる疑似ランダム順列に対して、本発明は特に有用

である。このやり方で幾つかの組を順列置換しなければならないときは、メモリ内の 1 つの組からのデータ項目は、それが読み出されるのに伴って新しい組のデータ項目と置き換える。この場合には、毎回基本的順列の結合を生成するごとにによりメモリに対するアドレスを生成する必要が生じる。上記計算手段はこの目的に極めて適している。従つて、本発明による回路配置の一実施例では、メモリを有して成り、 $m$  個の番号の組に属するところの番号は該メモリ中のそれぞれの位置を表すアドレスに対応し、また、各特定のサイクルでそれぞれ一組のデータ項目をメモリに書き込み、該特定のサイクルに後続する逐次サイクルの 1 つで上記それぞれ一組のデータ項目をメモリから読み出し／書き込み

ユニットを有して成り、上記それぞれ一組のデータ項目はその特定サイクル用に生成された順列に対応するアドレスの順番で書き込まれ、後続サイクル用に生成された順列に対応するアドレスの順番で書き込まれることを特徴とする。

本発明による回路配置の一実施例では、上記特定サイクル用に計算された順列の逆順列と上記後続サイクル用に計算された順列との結合が、該特定サイクルとは独立の通常の順列に等しくなるように、整係数行の組が選定される。このやり方で各組内のデータ項目は同じ疑似ランダム順列により順列置換される。

データ項目の疑似ランダム順列は、既り防護符号と組み合わせて使用するならば、特に有用である。このやり方は、送出又は記憶されようとするデータ項目であつて、後に受信又は検索されようとするデータ項目が、誤りに対して強固であることを許容する。

本発明はまた、 $m$  個の項目の一団を処理する方法を提供し、該方法は：該一団の各項目がその一団中の第 1 順位番号に従つて受け取られるところの該一団を受け取る段階；各特定の項目に、該特定の項目の上記第 1 順位番号の第 1 開数に従つて、記憶媒体内のそれぞれの位置を割り当てる段階；各特定の項目を、記憶媒体内でそれに割り当られたそれぞれの位置に記憶する段階；第 2 順位番号を、記憶位置の第 2 開数に従つて各記憶位置に割り当てる段階；記憶媒体から項目を検索する段階；及び、特定の記憶位置に割り当てる段階；記憶媒体から項目を位置の第 2 順位番号に従つて処理する段階；を含んで成る方法であつて、更に該方法は、 $n_1$  を順位番号とし； $n_2$  を記憶位置の順序での記憶位置の位置番号とし

;  $f_i$  及び  $g_i$  ( $i=0, \dots, s$ ) を各々が  $(s+1)$  個の整数から成るそれぞれの集合に属する整係数とし;  $\alpha$  を  $m$  のすべての素因数で整除される整数の番号とし、 $\alpha$  は  $m$  に關し  $s$  に等しいボテンシーを持つとするとき、上記第1関数及び第2関数はそれぞれ、

$$\text{location}(n1) = r_0 + \sum_{i=1}^s r_i \begin{bmatrix} f_1 \\ \vdots \\ f_i \\ \vdots \\ f_{s+1} \end{bmatrix}_{\alpha^{i-1}} \bmod m$$

この方法によれば、項目の順番は、記憶媒体を使用することにより順列置換がなされ、それらの項目は記憶媒体内のそれらの位置に従って取り扱われる。種々の異なる順列と、それらの結合と、それらの逆順列とは、同じ  $\alpha$  に対する上記公式を共に満足させる2つの異なる順列に従って、それぞれ記憶し検索することにより、容易に実現できる。茲でいう項目とは例えばデータ項目であるが、他の物理的項目、例えば製造工程中の製品であつて、システムティックな製造過程の影響を排除しようと欲するときにも適用できるであろう。それは例えば1つの工程から来る半製品を、利用可能な組立て装置のうちの1つに、システムティックに結び付けることを防止しようと欲するとき等である。

以下に、図面を引用して本発明及びその利点を詳細に説明する。

図1は、順列ユニットを示す図である。

図2は、伝送システムを示す図である。

図3は、アドレス生成器を示す図である。

図4は、モジュロ加算器を示す図である。

図1は、本発明による回路配置用の順列ユニットを示す。この順列ユニットは入力1と出力2とを有し、これらはいずれも読み出し／書き込み手段3に結合する。この読み出し／書き込み手段3はメモリ5に結合する。上記順列ユニットは

更にアドレス生成器7も有し、それはメモリ5のアドレス入力に結合する。

この順列ユニットはクロック(図示されていない)の制御の下に動作する。各クロックサイクルの間に、読み出し／書き込み手段3は、メモリ5から、すなわち当該サイクル用にアドレス生成器7の生成したアドレスを持つ位置から、1つデータ項目を読み出す。引き続いて読み出し／書き込み手段3は、当該サイクル用に入力1で受け取ったデータ項目を、この位置に書き込む。

その次のクロックサイクルの間に、メモリ5に対し別のアドレスについてこれが繰り返される。こうして、メモリ5の各位置からそれぞれのデータ項目が逐次読み出されて、出力2に与えられる。これらのデータ項目が一緒にになって出力2上のデータ項目のブロックを構成する。更にまた、入力上で受け取ったブロック中の各データ項目が、メモリのそれぞれの位置に書き込まれる。

これが引き続きブロックについて繰り返され、アドレス生成器7はメモリの全アドレスを生成する。こうして、各ブロックは逐次メモリに書き込まれ、再びメモリから読み出される。アドレス生成器はこれらのアドレスを自分自身の順序で生成する。従って各ブロックのデータ項目は、書き込まれたときの序列とは異なる序列で読み出される。

この順列ユニットは、例えば誤り訂正符号を用いる伝送システムでインターパーク器(interleaver)又はディンターリーパーク器(deinterleaver)として、使用される。

図2はそのような伝送システムを示す。このシステムは符号器10、インターパーク器12、変調器14、伝送チャネル、復調器16、ディンターリーパーク器18、及び符号器20を含む。

動作中にデータは符号器10の入力に与えられる。符号器はこれらのデータを誤り訂正符号で符号化する。すべての既知の誤り訂正符号が、例えば置込み符号又はターが符号(turbo code)が、この目的に使用できる。符号化されたデータはブロックに分割されて、その各々がシンボルの論理系列(logic succession)を含む。

符号器20は符号器に応するもので、符号器10から復号器20への伝送中に生じ

たシンボル誤りを訂正する。誤り訂正符号は論理系列内に亘り分散して生じるシンボル誤りを適切に訂正できるものである。バースト誤り、すなわち論理系列中の多数の連続したシンボルが正しくないという誤りについては、寧ろたやすく訂正し難い。

変調器14は、同時に送出される多数の周波数チャネルを持つ信号を生成する。各ブロックのシンボルは多数のグループに更に分割される。各グループは1つの周波数チャネルに対応し、1グループ内の複数のシンボルの情報は、対応する周波数チャネルで伝送される。このことは、例えば各グループのシンボルを1つの番号として翻訳し、これらの番号を1つの数列に並べて、この数列のFFT(高速フーリエ変換)を形成することにより、実現できる。次いでこのFFTの結果は伝送チャネル、例えば無線地上放送チャネル、を介して送出される。このFFT変換及び送出は後続のブロックに対し繰り返される。このことはそれ自身既知の0FFM(直交周波数分割マルチブレクシング)技術に対応する。

復調器16は変調器14に対応する。復調器は種々の周波数チャネルを同時に受信して、その各々がそれぞれの周波数チャネルで送られて来たシンボルのグループを再構築する。OFDM技術によれば、受信した信号の逆FFTを形成し、番号を再構築し、それからグループを再構築することにより、このことは実現される。インターリーブ器12は、論理系列内で互いに直接前後して並んだシンボルが殆ど常に異なる周波数チャネルで変調される、ということを保証するのに使われる。これらのチャネル(中間周波数のチャネルについて云えば)は0より寧ろ大きいことが、従って隣のシンボルが隣のチャネルではない処に入るようにするのが好適である。このことは、1つのチャネル又は隣合った複数のチャネルが崩壊しても論理系列中にバースト誤りを引き起こさないことを保証するのに役立つ。

インターリーブ器18はインターリーブ器12に対応するもので、逆動作を行うことにより論理系列が、復号器20に与えられる前に(シンボル誤りを除いて)順番を再構築される。

インターリーブ器12は、論理系列中で互いに並んでいる各1対のシンボルを、複数のチャネルの距離だけそれ互いに離して配列する。これらの距離はその

値がそれぞれ異なり、異なる距離は近似的に等しい頻度で起きることが保証されている。その結果、周波数チャネルの周期的システムで低品質の受信につながる伝送チャネルの崩壊に抵抗し得る。(茲で周期的システムとは、低品質の受信が周波数の関数として毎回同数のチャネルの後で自身反復するシステムを意味するものと理解する。)

それ以外の各1対のシンボルで、そのような1対のシンボル中の同時隙りがバースト誤り訂正の問題を起こし得るような互いにかなり接近しているシンボル対は、やはり複数のチャネルの距離だけそれ互いに離して配列する。これらの距離もやはりその値がそれぞれ異なるのが好適であり、異なる距離はやはり等しい頻度で起きることが保証される。

伝送チャネルは実例を用いて示される。本発明から逸脱することなく他のチャネル変調技術を用いることもできよう。

順列群 $\Lambda_\alpha$

アドレス生成器7により各ブロックに対しメモリ5のアドレスがその中に生成されるところのそれぞれの数列(sequences)は、各ブロックのデータ項目の順序をどのようにして入れ換えるかを定める。本発明は、mを1つのブロック中のデータ項目の数とし、 $\sigma(i)$  ( $i$ は異なる)に対しても互いに異なるとするとき、数列 $(\sigma(0), \sigma(1), \dots, \sigma(m-1))$ 中のアドレス $\sigma(i)$ を利用する。このような数列を順列と称し、 $\sigma$ という記号で表す。本発明は、二項係数

$$\left[ \begin{matrix} n \\ i \end{matrix} \right] = \frac{n(n-1)\dots(n-i+1)}{i!}$$

を用いて、 $\Lambda_\alpha$ を

$$\Lambda_\alpha = \{ (\sigma(0), \sigma(1), \dots, \sigma(m-1)) : \sigma(n) = x_0 + \sum_{i=1}^n x_i \left[ \begin{matrix} n \\ i \end{matrix} \right]_{\alpha^{i-1}} \bmod m \}$$

と定義するとき、集合 $\Lambda_\alpha$ の一部を形成する順列 $\sigma$ を特に顯著に利用する。茲で $\alpha$ は、mの任意の素因数で整除され、またmが4で整除されるならば4でも整除されるように選定する。例えばmが100(素因数は2と5)とすれば、 $\alpha$ は20の任意の倍数とすることができます。sは $\alpha$ の「ポテンシー」"potency"すなわち：

$$\alpha \cdot s = 0 \pmod{m}$$

となる最小の自然数である。従つて上の例では、 $\alpha = 20$ であれば、 $\alpha^2 = 400$ は $m = 100$ で整除されるから、 $s$ は2である。 $\alpha$ が $m$ のすべての素因数を1回だけ含むならば、そのときこの $\alpha$ は可能な限り最大のボテンシー $s$ を持つ。そのボテンシー $s$ は $m$ の素因数のうちで最大の幕を持つことの値に等しい。例えば、 $m = 45 = 3 \cdot 3 \cdot 5$ 、 $\alpha = 15 = 3 \cdot 5$ とするとき、最高のボテンシー $s = 2$ を持つ、それは素因数3が $m$ のうちで最大の幕の値(2)を持つからである。従つて、最小でもボテンシーが2の $\alpha$ を求めるためには、 $m$ は少なくとも1つの素数の平方で整除されなければならない: 素数である $m$ の値は、ボテンシーが2又はそれより大きいことは許容されないし、異なる素数の積となることも許容されない。それ故に $m$ は、もしボテンシー2を持つ $\alpha$ が要求されるならば、例えば1, 2, 3, 5, 6-2\*3, 7, 10=2\*5等であることはできない。4もやはりボテンシーが2の $\alpha$ を許容しない。

従つて、ボテンシー $s$ が1より大きい $\alpha$ の値を、ゆとりをもつて選択することができるためには、 $m$ は適当に大きな数でなければならず、また多くの異なる素因数を含んでなければならない。有限のボテンシー $s$ を持つすべての $\alpha$ の値は、基本的な $\alpha$ の値の整数倍になるであろう。この基本的な $\alpha$ の値は、 $m$ のすべての素因数の積であり、可能な限り最高のボテンシーを持つ。

数 $f_i$ は、集合 $\Lambda \alpha$ からの $\sigma(i)$ 順列が0から $m-1$ に直るように選定された自然数である。(例えばすべての $i > 0$ に対して $f_i = 1$ であるか、又は $i > 0$ で $m$ と互いに素な $f_i$ と $m$ の最大公約数が1であるときには $f_i$ は独立であり;  $f_0 = 0$ であるときに、これは線形合同アルゴリズムから求めることのできる順列に対する順列を生成して最も良いものを選定することにより、最適化できる。)

集合 $\Lambda \alpha$ の内部で $\sigma(n)$ 多項式は数列の中のそれらの位置 $n$ に従属する。この多項式の次数は $\Lambda \alpha$ の内部では最大でも $s$ である。疑似ランダム順列に対しては $s$ は2次又はそれより高次であることが好適である。ランダム性は、種々の異なる順列を生成することにより、最適化できる。

次で集合 $\Lambda \alpha$ のエлементの積を定義する: 順列 $\sigma$ と $\pi$ の積 $\sigma \circ \pi$ とは、順列 $\sigma$ と順列 $\pi$ との結合である。すなわち

$$\Delta \pi(n) = \pi(n+1) - \pi(n)$$

$$[\Delta_i \pi(n)]_{n=0} = h_i \alpha^{i-1}$$

$$(\sigma \circ \pi)(n) = \sigma(\pi(n))$$

と定義する。集合 $\Lambda \alpha$ が、この積 $\circ$ が、この積 $\circ$ という算法に関して、群を構成する(数学的観念としての「群」を構成する)ことは証明できる。このことは、 $\Lambda \alpha$ が恒等順列を含むこと(すなわち $f_0 = 0$ ,  $f_1 = 1$ , 且つその他のすべての $f_i = 0$ ) ;  $\Lambda \alpha$ が恒等順列の2つの順列の結合は $\Lambda \alpha$ に属すること; 及び、 $\Lambda \alpha$ の任意の順列に対しその逆順列も $\Lambda \alpha$ に属すること; がすべて成り立つことを意味する。(これは、もし $m$ が4で整除されると $\alpha$ は4で整除されないようなら $\alpha$ に対しても成り立つし、またもし $\Lambda \alpha$ が順列に限定されなくとも成り立つ。)

積 $\sigma \circ \pi$ を記述する数 $f_i$ の計算は原理的には置換の問題である。順列 $\sigma$ と順列 $\pi$ とを、数 $g_i$ 及び数 $h_i$ を用いてそれぞれ次のように表すことにする:

$$\pi(n) = g_0 + \sum_{i=1}^s g_i \left[ \begin{matrix} n \\ i-1 \end{matrix} \right] \pmod{m}$$

$$\sigma(n) = g_0 + \sum_{i=1}^s g_i \left[ \begin{matrix} n \\ i-1 \end{matrix} \right] \pmod{m}$$

そうすると、積 $(\sigma \circ \pi)$ は、 $\sigma(n)$ を表す数式に置換 $\pi(n)$ を施すことにより計算できる、すなわち:

$$(\sigma \circ \pi)(n) = g_0 + \sum_{i=1}^s g_i \left[ \begin{matrix} \pi(n) \\ i-1 \end{matrix} \right] \pmod{m}$$

積 $\sigma \circ \pi$ を陽関数として表す数式は二項係数を計算することにより求められる。 $\Lambda \alpha$ が群を構成することから、この陽関数としての表現は、数行を自然数とすれば、次のように書き直すことができる:

$$(\sigma \circ \pi)(n) = x_0 + \sum_{i=1}^s x_i \left[ \begin{matrix} \pi(n) \\ i-1 \end{matrix} \right] \pmod{m}$$

これらの自然数 $x_i$ はこの数式から、例えば差分を用いて計算できる。 $n$ の関数 $\pi$ ( $\Delta$ は順列)の差分 $\Delta \pi(n)$ は

$$\Delta \pi(n) = \pi(n+1) - \pi(n)$$

と定義する。 $\Lambda \alpha$ から順列置換を反復して施すことにより

と順列 $\pi$ との結合である。すなわち

が得られ、 $\pi(0) = f_0$ がやはり成立。同様にして積  $\sigma \circ \pi$  に対しても

$$(\Delta' (\sigma \circ \pi))_{n=0} = f_{i \cdot \alpha^{-1} - 1}$$

$(\sigma \circ \pi)(0) = f_0$  とが成立。これを積  $\sigma \circ \pi$  に対する陽関数に適用する

と、

数列  $f_i$  が求められる。従って  $m = 100$  且つ  $\alpha = 20$  とした実例で、 $\sigma(n)$  が  $g_0 = g_1 = g_2 = 1$  であるときには  $\sigma(0) = 1$ ,  $\sigma(1) = 2$ ,  $\sigma(2) = 23$ , ...,  $\sigma(23) = 84$  となり、更にそれから、 $\sigma(\sigma(0)) = 2$ ,  $\sigma(\sigma(1)) = 23$  及び  $\sigma(\sigma(0)) = 84$  となる。次いでこれから結合  $\sigma(\sigma(n))$  は  $f_0 = 2$ ,  $f_1 = 21$ ,  $f_2 = 2$  により特定される。同様にして計算すれば、 $\sigma(\sigma(\sigma(n)))$  が  $f_0 = 23$ ,  $f_1 = 61$ ,  $f_2 = 3$  により特定される。

順列  $\sigma$  の逆順列  $\pi$  は、例えば、 $f_i$  に対する数式から積  $\sigma \circ \pi = e$  に対する解を求めることににより求められる。又はその代わりに、 $\sigma_1 = \sigma$  とするときに、 $\sigma_n = \sigma \circ \sigma_{n-1}$  を順次  $n$  について計算して行つて  $\sigma_n$  が恒等順列となるに至る（これが可能なことは群の性質から保証されている）ならば；  $\sigma_{n-1}$  が  $\sigma$  の逆順列である。

数列  $f_i$  から出発すれば、 $\wedge \alpha$  からの順列は再帰的 (recursive) な手法で簡単に生成できる。

図 3 は再帰的アドレス生成器を示し、これは  $\alpha$  がボテンシール  $s=2$  を持つ場合に、 $\wedge \alpha$  からの順列を生成するものである。この図では破線で区切つてあるように、このアドレス生成器は 2 つのセクション A 及び B を含む。このセクション A は、第 1 レジスタ 20、第 1 加算器 22、第 1 初期化器 21、及び第 1 マルチプレクサー 23 を含む。第 1 レジスタ 20 の出力は該アドレス生成器の出力となる。この出力は第 1 加算器 22 の入力に結合する。第 1 加算器 22 の出力及び第 1 初期化器 21 は、第 1 マルチプレクサー 23 を介して第 1 レジスタ 20 の入力に結合する。

セクション B は第 2 レジスタ 24、第 2 加算器 26、第 2 初期化器 25、及び第 2 マルチプレクサー 27 を含む。第 2 レジスタ 24 の出力は第 1 加算器 22 のもう 1 つの入力に結合し、また第 2 加算器 26 の入力にも結合する。第 2 加算器 26 はまた、メモリ 28 からの入力信号をも受け取る。第 2 加算器 26 の出力及び第 2 初期化器 25 は、第 2 マルチプレクサー 27 を介して第 2 レジスタ 24 の入力に結合する。

図 4 は、モジュロ加算器 (modulo adder) の実施例を示す。加算器 22 及び加算器 26 はモジュロ加算器として構成される。図 4 は、2 進 (binary) 加算器 22a、減算器 22b、及びマルチプレクサー 22c を示している。モジュロ加算器 22 の入力は 2 進加算器 22a の入力を構成する。2 進加算器 22a の出力は減算器 22b 及びマルチプレクサー 22c に結合する。減算器 22b の出力はまた、マルチプレクサー 22c にも結合する。減算器 22b の (引き算での位から借りる) 借り出力 (borrow output) はマルチプレクサー 22c の制御入力に結合する。マルチプレクサーの出力はセクション B の出力を構成する。

2 進加算器 22a は動作中に入力信号の和を計算する。減算器 22b はこの和  $m$  を引き算する。もしこの引き算の結果が 0 より小さければ、マルチプレクサー 22c が、上記の和をただ送出する。もし引き算の結果が 0 より大きければ、減算器が、和ではなくて該引き算の結果を送出する。

図 3 のアドレス生成器は、データ項目クロック (図示されていない) と同期して動作する；このクロックは、データ項目が読みみ出され書き込まれると、その都度 1 バルスを出力する。レジスタ 20 及び 24 の内容はこのバルスに応じて更新される。1 つのロック内で  $n$  番目のデータ項目を処理している時ににおけるレジスタ 20 及び 24 の内容を  $u_n$  及び  $v_n$  と記すと、

$$u_{n+1} = u_n + v_n \mod m$$

$$v_{n+1} = u_n + d \mod m$$

が成り立つ。 $n=0$  に対するレジスタ 20 及び 24 の内容は初期化器 21、25 により初期化される。

それから、第 1 レジスタ 20、第 2 レジスタ 24 が  $f_0$ ,  $f_1$  に初期化され、メモリが第 2 加算器に  $f_2 \alpha$  を与えると、アドレス生成器は次の級数：

$$u(n) = f_0 + \sum_{i=1}^{n-1} f_i \left[ \frac{f_0}{\alpha} \right]_{\alpha^{-1}} \mod m$$

を生成するであろう。ボテンシールの高い方の  $\alpha$  値を用いるときは、セクション B のような複数のセクションがセクション A とセクション B の間に縦つなぎに (in cascade) 配置される。これらのセクション A, B 間に縦つなぎに配置されたセクションには、 $(A, B$  も含んで) 順番に  $i = 1, \dots, s-1$  と番号が付され、これら種

々のセクション中のレジスタは、 $f_{i-1}$ という直に初期化される。  
 $\wedge \alpha$ から順列を生成するのに用いられるもう1つの差分技術は、変形された差

分 $\Delta \alpha$ 、すなわち：

$$\Delta \alpha_i \alpha(n) = \alpha(n+1) - (1 + \alpha_i \lambda) \alpha(n)$$

と定義された $\Delta \alpha$ を利用する。もし $\sigma_i(n+1)$ がこの $\Delta \alpha_i \alpha(n)$ の式を用いて計算されようとするなら、掛け算が必要となる。しかしこれを適切に選定すれば、この計算に必要な再帰的なセクションの数は限定される。

順列群 $\wedge \alpha$ の応用

$\wedge \alpha$ の群としての性質から、順列の結合により得られた順列は再び $\wedge \alpha$ に属する順列の簡単な形に書ける。本発明は、疑似ランダム順列を実行するための簡単な順列ユニットの構築に、この様様を利用する。

最初の応用は、同じ順列 $\pi(n)$ を各ブロックで実行しようとした際に、この順列ユニットは、同じ順列 $\pi(n)$ を各ブロックのデータ項目を一連のアドレス $\sigma_i(n)$ に従って（すなわち先行のブロックのデータ項目が読み出されたシーケンス内に）書き込む。それに従って順列ユニットは一連のアドレス $\sigma_{i+1}(n)$ に従ってデータ項目を読み出す。すると、n番目のデータ項目として書き込まれたデータ項目は、 $\pi(n)$ 番目のデータ項目として読み出されなければならない。

これは、もし $\sigma_{i+1}(n) = \pi(\sigma_i(n))$ ならば、従って $\sigma_{i+1} = \pi \circ \sigma_i$ ならば成立。引き続くブロックの順列に対し、毎回 $\sigma_i$ を増しながらこれが繰り返される。 $\wedge \alpha$ からの順列 $\pi$ 及び $\sigma_i$ が用いられれば $\sigma_{i+1}$ も常に $\wedge \alpha$ に属することになる。その結果、すべての $\sigma_i$ が簡単に生成できる。この目的のために、例えば図3に示すアドレス生成器が使用され、又はその代わりに $\wedge \alpha$ からの順列のエレメントに対する順列が使用される。

2番目の応用は、引き続くブロックに対し異なる順列 $\pi_i(n)$ 、 $\pi_{i+1}(n)$ を実行

することに関する。そのときは $\sigma_{i+1}(n) = \pi_i(\sigma_i(n))$ が成立している。もし順列 $\pi_i(n)$ 、 $\pi_{i+1}(n)$ が同じ $\wedge \alpha$ から選ばれているならば、一連の $\sigma_i$ もまた $\wedge \alpha$ からの順列となり、簡単に生成できる。

反対に、もし $\sigma_i$  ( $i=1, \dots$ ) がすべて1つの集合 $\wedge$ のエレメントとして選ばれ

ているならば、順次ブロック $j$ に対する順列 $\pi_j$ 及びその逆順列はその $\wedge$ のエレメントであることが保証され、簡単に生成できる。これは例えば、出力2から送出されたデータ項目“n”がどのように順列置換されたかを信号する必要があるとき、すなわちこのデータ項目を入力1が受け取ったときにブロック $j$ 内のその位置 $\pi_{j-1}(n)$ を信号する必要があるときに、応用できる。 $\pi_{j-1}(n)$ が $\wedge$ のエレメントであるという事実を用いれば、一連の $\pi_{j-1}(n)$ が、nの引き続く値に対して簡単に生成できる。

これは、疑似ランダム順列 ( $\alpha$ の最高次数に対する係数 $f_i$ が0でない) と恒等順列 ( $\sigma(n) = 0, 1, \dots, m-1$ ) が $\sigma_i$ として交互に使われるときにも当てはまる。（結果として得られる順列 $\pi$ ）が疑似ランダムであるためには、少なくとも1つ置きに順列 $\sigma_i$ が疑似ランダムであることが必要で、すべての $\sigma_i$ がランダムであるには及ばない。）適切に選択された $\sigma_i$ に対して、これは各ブロックにおける引き続くアドレス間の差がほぼ均等に分布するインターリービングをもたらす。確かに2つの異なる順列のみを使用することはインターリービングを簡単なものにする。

順列 $\pi_i(n)$ 及び順列 $\pi_{i+1}(n)$ が異なる集合 $\wedge \alpha$ 及び $\wedge \alpha'$ から選択されるときは、両方を含む $\wedge \alpha''$ が求められることになり、茲では $\alpha''$ が $\alpha$ と $\alpha'$ の最大公约数を構成し；そうすると $\alpha''$ のボテンシーは $\wedge \alpha$ 及び $\wedge \alpha'$ のそれよりも高くなるであろう。すると $\sigma_i$ を書き込み、読み出すのに必要なシーケンスは $\wedge \alpha$ に属し、従って簡単に生成できる。

シーケンス $\sigma_i$ を記述する番号 $f_i$ （ $i=1, \dots, m-1$ ）は、上記の順列の結合を表す順列を用いて計算できる。しかしこ多くの場合にこれらの番号は再帰的に計算できることが判っている。もし $\alpha$ のボテンシー $s$ が2ならば、

$$f_0(n) = c, \quad f_1(n) = b, \quad f_s(n) = e$$

とするときに：

することに関する。そのときは $\sigma_{i+1}(n) = \pi_i(\sigma_i(n))$ が成立している。もし順列 $\pi_i(n)$ 、 $\pi_{i+1}(n)$ が同じ $\wedge \alpha$ から選ばれているならば、一連の $\sigma_i$ もまた $\wedge \alpha$ からの順列となり、簡単に生成できる。

$$f_0^{(i+1)} = f_0^{(i)} + c f_1^{(i)} + [c(c-1)/2] \alpha f_2^{(i)}$$

$$f_1^{(i+1)} = b f_1^{(i)} + (b c + b(b-1)/2) \alpha f_2^{(i)}$$

$$\alpha f_2^{(i+1)} = \alpha c f_1^{(i)} + (b b + \alpha(\alpha-1)/2) \alpha f_2^{(i)}$$

が成り立つ（これらの式はすべてmodulo mとする）。

本発明は図1及び図2に示す回路配置に応用できる。この回路配置は一連のデータ項目のブロックを受け取り、これらのブロックを出力するための順列ユニットを含み、各ブロックのデータ項目は順列置換された形で出力される。茲で順列ユニットは、

— メモリヒ：

— データ項目をメモリに書き込み、またメモリから読み出された位置のそれをメモリに読み込み、またメモリから読み出された位置のそれをデータ項目がメモリに書き込まれ、またメモリから読み出された位置のそれをデータ項目がメモリに書き込まれる。するとデータ項目を読み出すことにより実行できる。もし $\alpha$ が少なくて2で且つ $\alpha$ の非0の最大幕の係数 $f_0$ が0でないならば、これらの順列は疑似ランダムな性格を持つであろう。アドレス生成器は常に同じのままである。アドレス生成器は例えば再帰的な回路を用いて実現できる。このやり方で最も簡単な疑似ランダム順列を生成する方法はボテンシーアルゴリズムである。その式はそのとき順列を生成するのに必要な計算の数が最少だからである。しかし、ボテンシーアルゴリズムは、そのとき順列を生成するのに必要な計算の数が最も多くなる。

この回路配置では、上記アドレス生成器は各ブロックに対してそれぞれのアドレス列を生成するように配置され、該アドレス列では、各 $n$ に対し $n$ 番目のアドレスが：

$m$ をブロック内のデータ項目の数とし； $\alpha$ を $m$ のすべての素因数で整除され、ボテンシーアルゴリズムは2か又はそれ以上の整数とし； $f_i$  ( $i=0, \dots, s$ ) をブロックが変われば常に変わるものとするとき、次の関係式：

$$\alpha(n) = x_0 + \sum_{i=1}^s x_i [f_i]_{\alpha^{-1}} \bmod m$$

に一致するところの、番号 $0, \dots, m-1$ の順列 $\alpha(n)$ に対応する。

$m$ が4の倍数なら $\alpha$ は4の倍数であることが好適である。また、アドレス生成

器は、アドレス列を生成するための再帰ユニットと、或るブロックに対しアドレス列を生成する前に再帰ユニットを初期化するための初期化手段とを有することが好適である。簡単な順列を得るために、ボテンシーアルゴリズムは2であり、 $n$ は0を除きすべての $f_i$ が等しく且つ $m$ との最大公約数は1であることが好適である。この回路配置の1つの応用では、順列ユニットの動作は各ブロックに対しそれぞれの順列をもたらし、その順列は書き込むときのアドレス列を当該ブロックの読み出すときのアドレス列に関連させ、 $f_i$  ( $i=0, \dots, s$ ) はすべてのブロックに対しそれぞれの順列が同一であるように選定されているものである。

本発明が集合 $\Lambda$ の群としての性質から導かれていることは明らかである。データ項目のブロックが毎回この集合からの順列に従って順列置換されるときには、そのような動作はデータ項目の順列と一致するアドレス列内のメモリに毎回書き込み、統いてこの集合からの別の順列と一致してメモリからこれらのデータ項目を読み出すことにより実行できる。もし $\alpha$ が少なくて2で且つ $\alpha$ の非0の最大幕の係数 $f_0$ が0でないならば、これらの順列は疑似ランダムな性格を持つであろう。アドレス生成器は常に同じのままである。アドレス生成器は例えば再帰的な回路を用いて実現できる。このやり方で最も簡単な疑似ランダム順列を生成する方法はボテンシーアルゴリズムである。その式はそのとき順列を生成するのに必要な計算の数が最少だからである。しかし、ボテンシーアルゴリズムは常に高い $\alpha$ 値、例えばボテンシーアルゴリズムは、更によいランダム性を更に容易に実現できるから望ましい、という場合もある。それは選択の問題である：生成されたアドレス列を試験して、当該の応用に必要なランダム性を持つかどうかが判断されることになる。

本発明が、例として示した伝送システム又はもとと一般的にはアドレス生成器に限定されるものではない、ということは明らかであろう。基本的な疑似ランダム順列の結合である幾つかの疑似ランダム順列を生成しなければならない任意の利用分野に本発明は当てはまる。本発明は、図3に示すような同じ基本的生成器を用い、レジスター23, 27及びメモリ28を各特定の順列を規定する特定の値に初期化することにより、これら幾つかの順列を生成するのに用いられる。適切にプロ

グラムされたコンピュータを用いてもこれを達成できることは勿論であって、そこでは一組の係数 $\alpha$ で特定されるような異なる順列を生成するのに同じプログラム符号が用いられる。

本発明はまた、メモリに記憶されたデータ項目の一組の項目に適用でき、それは該一組の順列置換の方法は、任意の物理的種類の一組の項目に適用でき、それは該一組の項目を記憶媒体に記憶させ、その記憶媒体中の位置によりそれらの項目の処理の順序を定める。記憶と検索のそれぞれに同じ群 $\Lambda$ の異なる順列を用いる。このことは、記憶媒体から前のー組の項目が完全に検索される前に次のー組の項目を記憶するとき、更に複雑な順列を必要とせずに記憶媒体中のスペースの節約を可能にする。このー組の項目が、送出することにより処理されるデータ項目であつてもよいが、例えば製造工程で処理される製品であつてもよいのである。

【図 1】

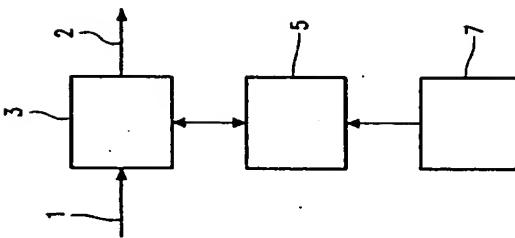


FIG. 1

【図 2】

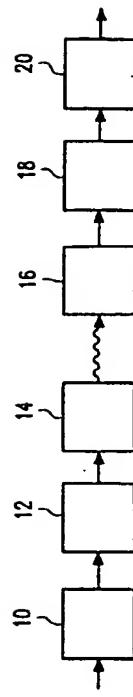


FIG. 2

(25)

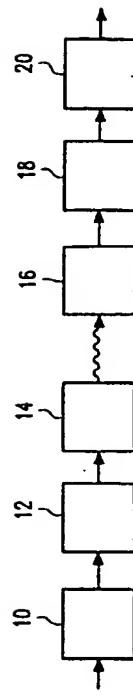


FIG. 2

【図 3】

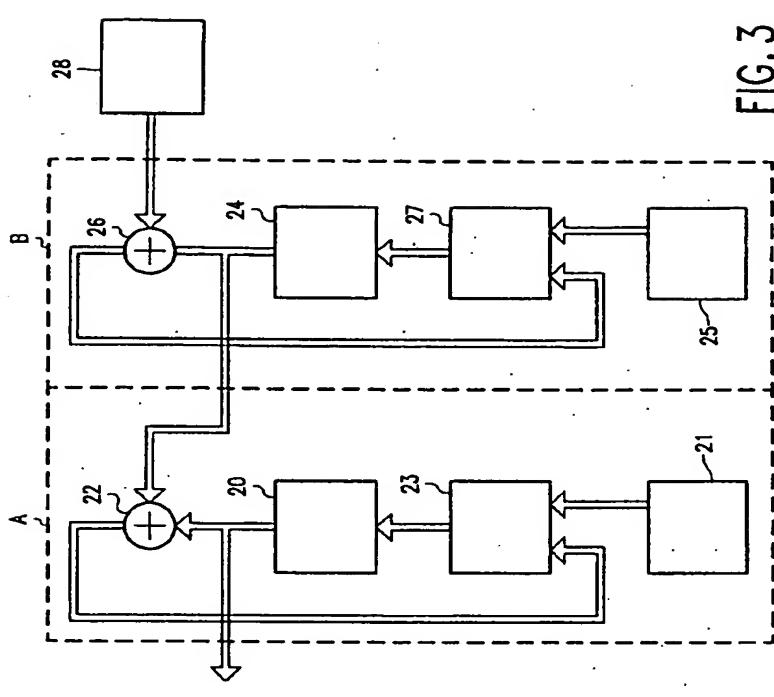


FIG. 3

[図4]

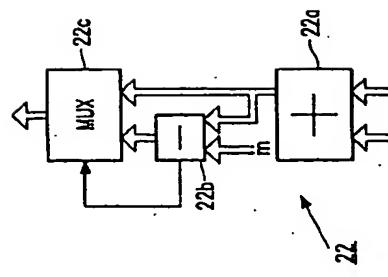


FIG. 4

## 【国際調査報告】

## INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB 96/00077

## A. CLASSIFICATION OF SUBJECT MATTER

IPC6: G06F 7/58

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: G06F, H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## EPODOC

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0406017 A1 (INDEPENDENT BROADCASTING AUTHORITY), 2 January 1991 (02.01.91), see whole document	7-16
Y	US 4547887 A (S.Y. MUI), 15 October 1985 (15.10.85), see whole document	7-16

<input type="checkbox"/>	Further documents are listed in the continuation of Box C.	<input checked="" type="checkbox"/> See patent family annex.
*	Special categories of cited documents	

\* A document defining the general state of the art which is not considered to be of particular relevance

\* B document but published on or after the international filing date

\* C document which may throw doubt on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

\* D document referring to an oral disclosure, use, exhibition or other means

\* E document published prior to the international filing date but later than the priority date claimed

\* F later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

\* G document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

\* H document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

\* I document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 July 1996	25-07-1996
Name and mailing address of the ISA: Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. + 46 8 666 02 86	Authorized officer Rune Bengtsson Telephone No. + 46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

## INTERNATIONAL SEARCH REPORT

International application No.  
PCT/IB 96/00077

## Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1.  Claims Nos.: 1-6  
because they relate to subject matter not required to be searched by this Authority, namely:  
Rule 39.1
2.  Claims Nos.:  
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3.  Claims Nos.:  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

## Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1.  As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2.  As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3.  As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4.  No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

## Remark on Protest

The additional search fees were accompanied by the applicant's protest.  
 No protest accompanied the payment of additional search fees.

**INTERNATIONAL SEARCH REPORT**  
Information on patent family members

01/07/96

International application No.  
PCT/IB 96/00077

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP-A1- 0406017	02/01/91	AU-A- 5942390 WO-A, A- 9100672	17/01/91 10/01/91
US-A- 4547887	15/10/85	NONE	

Form PCT/ISA/210 (patent family annex) (July 1992)

---

フロントページの続き

(31) 優先権主張番号 95200580.9  
(32) 優先日 1995年3月9日  
(33) 優先権主張国 オランダ (N L)  
(31) 優先権主張番号 95200642.7  
(32) 優先日 1995年3月16日  
(33) 優先権主張国 オランダ (N L)  
(81) 指定国 E P (A T, B E, C H, D E,  
D K, E S, F R, G B, G R, I E, I T, L U, M  
C, N L, P T, S E), J P, K R

【要約の続き】

団を疑似ランダム的に順列置換し、前の一団が完全にそれから検索されてしまう以前に上記項目の一団を該記憶媒体中に記憶させ始めることを可能にする。